UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,385	01/06/2004	Hashem M. Ebrahimi	1565.066US1	6809

21186 7590 02/12/2007

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/752,385	EBRAHIMI ET AL.	
	Examiner	Art Unit	
	Canh Le	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☒ Claim(s) *4-5* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 January 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/06/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Drawings

The drawings are objected to because on page 15, lines 17-26, "external client 420" does not match with Figure 4. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The disclosure is objected to because of the following informalities: On page 15, lines 17-26, "external client 420" does not match with Figure 4. Appropriate correction is required.

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

In claims 4 and 5, "the external client to activate one or more external reference links from a World-Wide Web (WWW) browser page" does not have support in the specification.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 4-8, 11, 13, 16-17, and 22-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Subramaniam et al. (US Patent: 6,081,900).

Claim 1

Subramaniam discloses a method to manage secure communications, comprising:

establishing a secure session on a secure site with an external client that communicates from an insecure site (Col.3 lines 35-50; Col.3, line 66 to Col.4 line 17);

detecting access attempts during the session directed to potentially insecure transactions (Col. 6, lines 40-49; By checking the IP address which the request was made, the target server 104 determines that the request (i.e. potentially insecure transactions) came from outside the security parameter 102); and

transparently managing the access attempts by inspecting the access attempts before making them available to the external client (Col. 6, lines 40-49).

Claim 2

Subramaniam discloses the method of claim 1 wherein the detecting further includes translating non-secure links into secure links for the insecure transactions before presenting results of the access attempts to the external client (Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)).

Claim 4

Subramaniam discloses the method of claim 1 further comprising:

identifying the potentially insecure transactions (Col. 6, lines 40-49; By checking the IP address which the request was made, The target server 104 determines that the request (i.e. potentially insecure transactions) came from outside the security parameter 102) as attempts by the external client to activate one or more external reference links from a World-Wide Web (WWW) browser page, wherein the external reference links

are associated with external sites not controlled by the secure session and not secure; and

using a proxy (Col.5, lines 42-49; One or more of the servers 104, 106 may be configured a wide variety way to operate as proxy server) on behalf of the external client during the secure session in order to access the external sites and making transactions with the external sites appear secure to the external client during the secure session (Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)).

Claim 5

Subramaniam discloses the method of claim 1 further comprising:

identifying the potentially insecure transactions as attempts by the external client (Col. 6, lines 40-49; Checking the IP address which the request was made, The target server 104 determines that the request (i.e. potentially insecure transactions) came from outside the security parameter 102) to activate one or more external reference links from a World-Wide Web (WWW) browser page, wherein the external reference links are associated with external sites not controlled by the secure session;

inspecting content or metadata of the content associated with the external reference links in advance of providing the external reference links to the external client (Col. 6, lines 46-60; A target server check user permissions against access control lists).

taking zero or more actions based on the inspection before the external reference links are visible, if at all, to the external client during the secure session (Col. 6, lines 61-67; Col. 7, lines 1-35; A border server 106 redirects a request from client a 112) .

Claim 6

Subramaniam discloses the method of claim 5 wherein the taking of the zero or more actions further includes at least one action that is at least one of:

issuing alerts (Col. 11, lines 61-67), notifications (Col. 8, lines 40-57), or advisories to a monitoring entity or log.

Claim 7

Subramaniam discloses the method of claim 5 wherein the inspecting the content further includes using a proxy (Col. 5, lines 38-49; One or more server 104, 106 may be configured a proxy servers) on behalf of the external client during the secure session for performing the inspecting.

Claim 8

Subramaniam discloses a method to manage secure communications, comprising:

detecting potentially insecure transactions occurring during a secure session, wherein the insecure transactions result from actions requested by an external client participating in the secure session (Col. 6, lines 40-49; By checking the IP address

which the request was made, the target server 104 determines that the request (i.e. potentially insecure transactions) came from outside the security parameter 102);

inspecting the potentially insecure transactions in advance of satisfying the actions requested (Col. 6, lines 46-60; A target server check user permissions against access control lists); and

making a determination for at least one of the following: permitting the insecure transactions to proceed unmodified by performing the actions requested for the external client, permitting the insecure transactions to proceed in a modified fashion (Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)), and denying the insecure transactions by denying the actions requested.

Claim 11

Subramaniam discloses the method of claim 8 wherein the inspecting further includes, identifying the potentially insecure requests as an external client access attempt to reference an external site outside the control of the secure session (Col. 6, lines 46-49).

Claim 13

Subramaniam discloses the method of claim 11 wherein the making a determination further includes permitting the insecure transactions to proceed in a **modified fashion** by transparently processing the external client access attempt within a proxy making the external client access attempt appear to be part of the secure

session (Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)).

Claim 16

Subramaniam discloses a secure communications management system, comprising:

a secure communications manager (Figure 1, box 102) that manages a secure session with an external client associated with an insecure site; and

a proxy (Col. 5, lines 42-49) that interacts with the secure communications manager in order to inspect potentially insecure communications requested by the external client during the secure session, and wherein the proxy selectively processes the potentially insecure communications on behalf of the external client within the secure session.

Claim 17

Subramaniam discloses the secure communications manageme333nt system of claim 16 wherein the secure communications manager translates Hypertext Transfer Protocol (HTTP) insecure communications into HTTP over Secure Sockets Layer (HTTPS) secure communications during the secure session (Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)).

Claim 22

Subramaniam discloses a secure communications management system, comprising:

a secure session (Col. 3, lines 34-51; Col. 3, line 66 to Col. 4, line 8); and

secure reference links accessible within the secure session (Col. 3, lines 34-51; Col. 3, line 66 to Col. 4, line 8); and potentially insecure reference links accessible from the secure session;

wherein an external client associated with an external site establishes the secure session with a secure site, the external client references the secure reference links and the potentially insecure reference links during the secure session, and wherein the potentially insecure reference links are inspected and modified in advance of being made available to the external client during the secure session (Col. 3, lines 34-51; Col. 3, line 66 to Col. 4, line 8).

Claim 23

Subramaniam discloses the secure communications management system of claim 22 further comprising a proxy that inspects and modifies the potentially insecure reference links in advance of making them available to the external client during the secure session (Col. 5, lines 42-49; Col. 4, lines 5-8).

Claim 24

Subramaniam discloses the secure communications management system of claim 22 wherein the secure session is represented within a Word-Wide Web (WWW) browser that the external client uses for interacting with the secure site (Col. 7, lines 4-11).

Claim 25

Subramaniam discloses the secure communications management system of claim 22 wherein the potentially insecure reference links are transparently modified into a number of the secure reference links before being made available to the external client during the secure session (Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)).

Claim 26

Subramaniam discloses the secure communications management system of claim 22 wherein a number of the potentially insecure reference links are processed by a proxy on behalf of the external client and appear to the external client to be a number of the secure reference links (Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 3, 9-10, 12, 14-15, 18-21, and 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Subramaniam et al. (US Patent: 6,081,900) in view of "Netscape Proxy Server Administrator's Guide Version 3.5 for Unix", 1997, as provided by applicant herein after Netscape_unix_v3.5.

Claim 3

Subramaniam discloses the method of claim 1 further comprising:

identifying the potentially insecure transactions (Col. 6, lines 40-49; Checking the IP address which the request was made, The target server 104 determines that the request (i.e. potentially insecure transactions) came from outside the security parameter 102) as attempts by the external client to view a World-Wide Web (WWW) browser page having insecure Hypertext Transfer Protocol (HTTP) reference links (Col. 6, line 61 to Col. 7 line 24) or File Transfer Protocol (FTP) reference links embedded therein, and wherein the reference links reside within the secure site; and

Subramaniam does not disclose to suppress normally occurring security warning messages associated with the reference links, preventing the external client from viewing the security warning messages.

Netscape_unix_v3.5 discloses to suppress normally occurring security warning messages associated with the reference links, preventing the external client from viewing the security warning messages (Chapter 10, pages 1-3; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be an empty text).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improve techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 9

Subramaniam discloses the method of claim 8 wherein the inspecting further includes, identifying the potentially insecure transactions as a request by the external client to access a World-Wide Web (WWW) browser page having embedded reference links to other browser pages that reside within an environment of the secure session (Col. 6, lines 40-49; Checking the IP address which the request was made, The target

server 104 determines that the request (i.e. potentially insecure transactions) came from outside the security parameter 102), wherein the reference links are modified.

Subramaniam does not disclose to suppress normally occurring security warning messages when the browser page is presented to the external client.

Netscape_unix_v3.5 discloses to suppress normally occurring security warning messages when the browser page is presented to the external client (Chapter 10, pages 1-3; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be an empty text).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improve techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 10

Subramaniam further discloses a method permitting the insecure transactions to proceed in the modified fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links to HTTP over Secure Sockets Layer (HTTPS) (Col. 3, lines 66-67; Col. 4, lines 1-8; Transforming non-secure URLs (i.e. HTTP) into secure URLs (i.e. HTTPs)).

Subramaniam does not disclose to suppress the security warning messages.

Netscape_unix_v3.5 discloses to suppress the security warning messages (Chapter 10, pages 1-3; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be an empty text).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improve techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 12

Subramaniam discloses the method as described in claim 11.

Subramaniam does not disclose a method permitting insecure transactions to proceed unmodified.

The background of the invention discloses a method permitting insecure transactions to proceed unmodified (Col. 2, lines 36-41).

Subramaniam and the background of the invention do not disclose permitting normally occurring security warnings to be presented to the client before satisfying the external client access attempt to reference the external site.

Netscape_unix_v3.5 discloses permitting normally occurring security warnings to be presented to the client before satisfying the external client access attempt to reference the external site (Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server

can be configured a custom message, which sends to an external client. A customized text message can be security warning messages).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify Subramaniam and the method of the background of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 14

Subramaniam discloses the method as described in claim 11.

Subramaniam does not disclose a method as described in claim 14.

Netscape_unix_v3.5 discloses the method of claim 11 wherein the making a determination further includes *denying the insecure transactions after determining that the external client access attempt is corrupted* and notifying the external client of the denial (Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are

suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 15

Subramaniam discloses the method as described in claim 11.

Subramaniam does not disclose a method as described in claim 15.

Netscape_unix_v3.5 further discloses the method of claim 11 wherein the making a determination further includes *denying the insecure transactions after determining that the external client access attempt is corrupted* and logging information about the external client access attempt (Chapter 13, pages 1-7).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 18

Subramaniam discloses the secure communications management system of claim 16 wherein the proxy selectively modifies a number of the potentially insecure communications (Col. 3, lines 34-51; Col. 3, line 66 to Col. 4, line 8).

Subramaniam does not disclose to suppress normally occurring security warning messages that the secure communications manager issues.

Netscape_unix_v3.5 discloses to suppress normally occurring security warning messages that the secure communications manager issues (Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 19

The background of the invention discloses the secure communications management system of claim 16 wherein the proxy selectively leaves a number of the potentially insecure communications unchanged (Col. 2, lines 36-41).

The background of the invention does not disclose to issue security warning messages to the external client.

Netscape_unix_v3.5 discloses a proxy sending security warning messages to the external client (Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be

configured a custom message, which sends to an external client. A customized text message can be security warning messages).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of the background of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 20

Subramaniam discloses the secure communication system as claimed in claim 16. Subramaniam does not disclose a proxy which selectively denies a number of the potentially insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log.

Netscape_unix_v3.5 discloses a proxy which selectively denies a number of the potentially insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log (Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt; Proxy error log messages include Catastrophe error, Failure, information log entry, warning flags, and security warning).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by

including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 21

Subramaniam discloses the secure communication system as claimed in claim 16. Subramaniam does not disclose a proxy selectively sending custom warning messages or explanations to the external client regarding a number of the potentially insecure communications.

Netscape_unix_v3.5 discloses a proxy which selectively issues custom warning messages or explanations to the external client regarding a number of the potentially insecure communications (Chapter 10, pages 1-3; Chapter 13, page 1; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be security warning messages).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 27

Subramaniam discloses the secure communications management system in claim 22.

Subramaniam does not disclose a feature in claim 27.

Netscape_unix_v3.5 discloses security warning messages associated with a number of the potentially insecure reference links are suppressed and not visible to the external client during the secure session (Chapter 10, pages 1-4; A proxy server can be configured a custom message, which sends to an external client. A customized text message can be an empty text; Suppressing outgoing headers).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 28

Same discussion as claim 27.

Claim 29

Subramaniam discloses the secure communications management system in claim 22.

Subramaniam does not disclose a number of the potentially insecure reference links generate notifications to external entities.

Netscape_unix_v3.5 disclose a number of the potentially insecure reference links generate notifications to external entities (Chapter 13, page 1; A proxy will issue a fatal error (i.e. catastrophe) if an outside agent causes cache files to become corrupt).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Claim 30

Subramaniam discloses the secure communications management system in claim 22.

Subramaniam does not disclose a number of the potentially insecure reference links generate written messages to a security log.

Netscape_unix_v3.5 disclose a number of the potentially insecure reference links generate written messages to a security log (Chapter 13, page 1).

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the system of Subramaniam of the invention by including the step of Netscape_unix_v3.5 because it would improved techniques for

managing secure communications, such that unnecessary security warnings are suppressed and security threats are more meaningfully communicated (the background of this application).

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

The Dusse (Pub. No.: US 20020068554 A1) discloses method and system facilitating web based provisioning of two-way mobile communication devices.

The Barton et al. (US Patent: 7,093,121 B2) disclose transferring data via a secure network connection.

The Jerger et al (US Patent: 6,473,800 B1) disclose declarative permission requests in a computer system.

The Grantges, Jr. (US Patent: 6,324,648 B1) discloses secure gateway having user identification and password authentication.

The Ioele et al. (US Patent: 7,007,299 B2) disclose method and system for internet hosting and security.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380.

The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
February 5, 2007

WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER